муниципальное бюджетное учреждение дополнительного образования
Железнодорожного района города Ростова-на-Дону

«Детско-юношеская спортивная школа № 5»

Согласовано:

На заседании научно-методического совета

Прот. № 1 от 25.08.2022 г.

Утверждено:

Директор МБУ ДО ДЮСШ № 5

_____

Приказ № 173 от 01.09.2022

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ДЛЯ ТРЕНЕРОВ-ПРЕПОДАВАТЕЛЕЙ

МБУ ДО ДЮСШ № 5

«Работа с родителями по обеспечению безопасной информационной среды»

(новая редакция)

Соловьева Н.И., Цуцкиридзе К.Г., Труфанов А.В., Цулая З.А.,Беляев АВ., Мартышенко Н.В., Пискарев Н.Н.

Ростов-на-Дону

2022

Введение

Согласно российскому законодательству ***информационная безопасность детей*** – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию").

Являясь активными пользователями различных медиа, дети и подростки, однако, не всегда понимают истинный смысл сообщений, мотивы и механизмы их создания. Одновременно стоит отметить, что информация, передаваемая по медиаканалам, направлена на манипулирование сознанием потребителя.

Если для взрослого человека, занимающегося делом, интернет – помощник и друг, то для детей – это большой соблазн и опасность. Самое главное для родителей и взрослых людей – обеспечить безопасный интернет для детей. Естественно, что в первую очередь, обеспечение безопасности интернета для детей ложится на родителей и людей, отвечающих за детей. Начнем рассмотрение темы с небольшого анкетирования. *Приложение 1*

К ***информации, запрещенной для распространения среди детей***, относится информация: 1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству; 2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; 3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом; 4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи; 5) оправдывающая противоправное поведение; 6) содержащая нецензурную брань и т.д.

Данные методические рекомендации предназначены для тренеров-преподавателей спортивной школы.

Работа с родителями по обеспечению

безопасной информационной среды

Работу с родителями по обеспечению безопасной информационной среды необходимо осуществлять во время проведения родительских собраний.

Проведение родительского собрания.

Родительские собрания целесообразно проводить по группам и уровням образования.

В начале родительского собрания рекомендуется провести анонимное анкетирование, которое позволит выявить отношение родительской общественности к внедрению в образовательный процесс ИКТ. По результатам анкетирования будет определена дальнейшая стратегия работы образовательной организации по безопасности детей в сети Интернет. После анкетирования проводится беседа по проблеме доступа ребенка к сети Интернет, в которой поднимаются наиболее актуальные вопросы (*Приложение 4, 5)*.

Далее даются рекомендации родителям по работе детей в сети Интернет (с учетом возрастных особенностей).

В конце родительского собрания всем родителям предлагается памятка по безопасности детей в сети Интернет при помощи программных средств *(см. Приложение 7,8)*.

Глобальная сеть: правила пользования. Линия помощи «Дети онлайн» представляет рекомендации для родителей

Как защитить ребенка от столкновения с вредоносной информацией в сети? Как научить его справляться с последствиями таких встреч?

Знакомства в Интернете

При общении в сети существует угроза подвергнуться рискам, связанным с контактами с другими людьми, не всегда знакомыми в реальной жизни. Особенно опасен груминг - установление дружеских отношений с ребенком с целью вступления в сексуальные отношения. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), преступник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга:

1. Будьте в курсе, с кем взаимодействует в Интернете Ваш ребенок. Старайтесь регулярно проверять список его контактов, чтобы убедиться, что он лично знает всех, с кем общается.
2. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать виртуальным знакомым свои фотографии.
3. Объясните ребенку, что при общении на ресурсах,

требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), нельзя использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.

4. Если ребенок интересуется контактами с людьми намного старше его, следует обратить на это внимание и провести с ним разъяснительную беседу.

5. Не позволяйте ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствие взрослого человека. Если ребенок желает встретиться с новым Интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

6. Интересуйтесь тем, куда и с кем ходит Ваш ребенок.

Кибербуллинг

Кибербуллинг – преднамеренное и протяженное во времени агрессивное поведение по отношению к жертве, осуществляемое одним человеком или группой людей посредством различных электронных сервисов.

Предупреждение кибербуллинга:

1. Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова-читать грубости так же неприятно, как и слышать.

2. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

3. Научите детей правильно реагировать на обидные слова или действия других пользователей.

4. Объясните детям, что информация, которую они выкладывают в Интернете, может быть использована против них.

5. Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования сетью.

Кибермошенничество

Кибермошенничество - один из видов киберпреступлений, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.) с целью причинить материальный или иной ущерб.

Предупреждение кибермошенничества:

1. Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться с взрослыми перед тем, как воспользоваться теми или иными услугами сети.

2. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.

Интернет-магазины:

– Ознакомьтесь с отзывами покупателей.

– Избегайте предоплаты.

– Проверьте реквизиты и название юридического лица — владельца магазина.

– Уточните, как долго существует магазин.

– Посмотреть можно в поисковике или по дате регистрации домена (сервис Whois).

– Поинтересуйтесь выдачей кассового чека.

– Сравните цены в разных Интернет-магазинах.

– Позвоните в справочную магазина.

– Обратите внимание на правила Интернет-магазина.

– Выясните, сколько точно вам придется заплатить.

Противозаконный и неэтичный контент

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки посторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду наркотиков и действий, причиняющих вред физическому и психическому здоровью. Столкнуться с рисками такого рода можно практически везде: сайты, социальные сети, блоги, торренты, видеохостинги. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Предупреждение столкновения с неэтичным или противозаконным контентом:

- установите на компьютер специальные программные фильтры (при нажатии на вылетающий баннер вместо страницы будет всплывать пустое окно) или специальные программы, называемые системами родительского контроля (они позволяют родителям решать, какое содержимое могут просматривать их дети);

- приучите ребенка советоваться с взрослыми и немедленно сообщать о появлении подобного рода нежелательной информации;

- объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Научите их спрашивать о том, в чем они не уверены;

- старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.

Вредоносные программы

Вредоносные программы – различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Они также способны снижать скорость обмена данными с Интернетом и

даже использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

1. Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Подобные программы наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

3. Периодически старайтесь полностью проверять свои домашние компьютеры.

4. Делайте резервную копию важных данных.

5. Старайтесь периодически менять пароли (например, от электронной почты), но не используйте слишком простые пароли.

Если ребенок все же столкнулся с какой-либо угрозой в сети, и она оказала на него негативное влияние.

Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.

Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и в какой степени это могло повлиять на ребенка.

Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате Интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации.

Выясните, что привело к данному результату — непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в Интернете.

Если ситуация связана с насилием в Интернете в отношении ребенка, то необходимо узнать информацию об агрессоре, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что

известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Жестко настаивайте на том, чтобы ребенок избегал встреч с незнакомцами, особенно без свидетелей.

Проверьте все новые контакты ребенка за последнее время.

Соберите наиболее полную информацию о происшествии как со слов ребенка, так и помощью технических средств — зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.

Если Вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, если ребенок недостаточно откровенен с вами или вообще не готов идти на контакт, если Вы не знаете, как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации и подскажут, куда и в какой форме обратиться, если требуется вмешательство психолога, полиции или других служб и организаций.

С более подробными рекомендациями Вы можете ознакомиться на сайте www.detionline.com

Приложение 1

Тесты-опросники на выявление ранних признаков компьютерной зависимости у несовершеннолетних

Тесты позволяют определить уровень компьютерной зависимости учащихся образовательных учреждений разной возрастной категории.

Тесты-опросники состоят из двух блоков: первый блок заполняется учащимися, второй – родителями учащихся.

Инструкция: Внимательно прочтите десять вопросов. Каждый из них Вы должны оценить как верный или неверный. Если вопрос кажется Вам верным или преимущественно верным, поставьте «Да», если неверным – «Нет».

Блок I. Тесты для учащихся образовательных учреждений Вариант 1.

1. Часто ли Вы замечаете, что проводите в он-лайн больше времени, чем намеревались? (да / нет)
2. Часто ли Вы пренебрегаете домашними делами, чтобы провести больше времени в сети? (да / нет)
3. Часто ли окружающие интересуются количеством времени, проводимым Вами в сети? (да / нет)
4. Замечете ли Вы, что Ваша успеваемость в школе стала хуже из-за того, что на учебу у Вас не остается времени, так как Вы слишком много времени проводите в сети? (да / нет)
5. Часто ли Вы представляете, как вновь окажетесь в Интернете? (да /

нет)

6. Часто ли Вы ощущаете, что жизнь без Интернета скучна, пуста и безрадостна? (да / нет)

7. Часто ли Вы ругаетесь, кричите или иным образом выражаете свою досаду, когда кто-то пытается отвлечь Вас от пребывания в сети Интернет? (да / нет)

8. Часто ли Вы пренебрегаете сном, засиживаясь в Интернете допоздна? (да / нет)

9. Чувствуете ли Вы оживление, возбуждение, находясь за компьютером? (да / нет)

10. Появились ли у Вас нарушения сна и/или изменился ли режим сна, с тех пор как Вы стали использовать компьютер ежедневно? (да / нет)

Вариант 2.

1. Вам приходилось просить учителей, родителей заменить хотя бы часть знаний компьютерными играми? (да / нет)

2. Вы чувствуете, что Вам не всегда удается сразу же прекратить компьютерную игру? (да / нет)

3. Вы чувствуете себя раздраженным или усталым, если долго не играете на компьютере? (да / нет)

4. Обычно Вы занимаетесь компьютерными играми больше, чем планировали? (да / нет).

5. Вам приходилось срочно закрывать окно с компьютерной игрой или сайта, когда приходили родители, учителя, друзья? (да / нет)

6. Вам приходилось садиться за компьютерную игру, чтобы исправить себе настроение (например, чувство вины, раздражительности) или просто, чтобы успокоиться? (да / нет)

7. Возникают ли у Вас головные боли после игры за компьютером? (да / нет) нет).

8. Пренебрегаете ли Вы приемом пищи из-за компьютерной игры? (да /

9. Пренебрегаете ли Вы личной гигиеной из-за компьютерной игры? (да / нет)

10. В обычной жизни чувствуете ли Вы пустоту, раздражительность, подавленность, которые исчезают при игре за компьютером? (да / нет)

Подсчет результатов: производится специалистами, проводившими тестирование.

«Да» – 1 балл,
«Нет» – 0 баллов.

Полученные баллы суммируются.

0 – 3 балла – низкий уровень компьютерной зависимости.

4 – 6 балла – средний уровень компьютерной зависимости.

7 – 10 баллов – высокий уровень компьютерной зависимости.

Блок II. Тесты для родителей

Вариант 1.

Ваш ребенок, …

1. Приходя домой, первым делом садится за компьютер? (да / нет)
2. Забросил домашние дела, учебу, стал непослушным? (да / нет)
3. Раздражителен, груб, если его отвлекают от компьютера? (да / нет)
4. Совершает прием пищи, не отрываясь от компьютера? (да / нет)
5. Не знает, чем себя занять, если компьютер недоступен или сломался? (да / нет)
6. Не способен контролировать время, проводимое за компьютером? (да / нет)
7. Тратит много денег на компьютерные игры? (да / нет)
8. Перестал общаться с друзьями, все больше времени проводит в он- лайн? (да / нет)
9. Посещает различные запретные сайты? (да / нет)
10. Постоянно говорит о компьютерных играх, об общении в Интернете? (да / нет)

Вариант 2.

Ваш ребенок, …

1. Испытывает раздражение при необходимости закончить игру? (да / нет)
2. Из-за компьютерной игры жертвует времяпровождением с семьей, родными? (да / нет)
3. После компьютерной игры жалуется на головные боли, возникает сухость слизистой оболочки глаз? (да / нет)
4. Высказывает желание проводить в Интернете больше времени? (да / нет)
5. Во время компьютерной игры полностью отрешается от реальной действительности, целиком переносясь в мир игры? (да / нет)
6. Из-за компьютерной игры пренебрегает питанием, личной гигиеной? (да / нет)
7. В результате систематического времяпровождения за компьютером, потерял интерес к учебе, к спортивным секциям,

кружкам? (да / нет)

8. Преимущественно находится в хорошем настроении, занимаясь компьютерными играми или общением он-лайн? (да / нет)
9. Проводя длительное время в Интернете, нарушает режим дня? (да / нет)
10. Предпочитает общение с виртуальными друзьями, чем с реальными? (да / нет)

Подсчет результатов: производится родителями.

«Да» – 1 балл,
«Нет» – 0 баллов.
Полученные баллы суммируются.

0 – 3 балла – низкий уровень компьютерной зависимости; родители могут справиться с возникшей проблемой самостоятельно (*см. рекомендации*);

4 – 6 балла – средний уровень компьютерной зависимости, для решения проблемы необходима консультация специалиста (психолога);

7 – 10 баллов – высокий уровень компьютерной зависимости, чрезмерное увлечение компьютером, которое может привести к психологической зависимости ребенка; родители не могут справиться с возникшей проблемой самостоятельно, поэтому необходимо обратиться за помощью к специалисту (психологу, психотерапевту).

Приложение 2

Анкета №1 «Осторожно, вирус!»

Что является основным каналом распространения компьютерных вирусов?
1. Веб-страницы
2. Электронная почта
3. Флеш-накопители (флешки)

Для предотвращения заражения компьютера вирусами следует:
1. Не пользоваться Интернетом
2. Устанавливать и обновлять антивирусные средства
3. Не чихать и не кашлять рядом с

компьютером Если вирус обнаружен,

следует:

1. Удалить его и предотвратить дальнейшее заражение
2. Удалить его и предотвратить дальнейшее заражение
3. Удалить его и предотвратить дальнейшее заражение
4. Установить какую разновидность имеет вирус
5. Установить какую разновидность имеет вирус
6. Установить какую разновидность имеет вирус
7. Выяснить как он попал на компьютер

Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
1. Применение брандмауэра
2. Обновления операционной системы
3. Антивирусная программа

Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
1. Уничтожение компьютерных вирусов
2. Создание и распространение компьютерных вирусов и вредоносных программ
3. Установка программного обеспечения для защиты компьютера

Анкета №2 «Осторожно, Интернет!»

Какую информацию нельзя разглашать в Интернете?
1. Свои увлечения
2. Свой псевдоним
3. Домашний адрес

Чем опасны социальные сети?
1. Личная информация может быть использована кем угодно в разных целях
2. При просмотре неопознанных ссылок компьютер может быть взломан
3. Все вышеперечисленное верно

Виртуальный собеседник предлагает встретиться, как следует поступить?
1. Посоветоваться с родителями и ничего не предпринимать без их согласия
2. Пойти на встречу одному
3. Пригласить с собой друга

Что в Интернете запрещено законом?
1. Размещать информацию о себе
2. Размещать информацию других без их согласия
3. Копировать файлы для личного использования

Действуют ли правила этикета в Интернете?

1. Интернет - пространство свободное от правил
2. В особых случаях
3. Да, как и в реальной жизни

Приложение 3

Круглый стол «Основы безопасности в сети Интернет»

Правила работы в сети Интернет:

1. Не входите на незнакомые сайты.
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4. Никогда не посылайте никому свой пароль.
5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
6. При общении в Интернет не указывать свои личные данные, а использовать псевдоним (ник).
7. Без контроля взрослых ни в коем случае не встречаться с людьми, с которыми познакомились в сети Интернет.
8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
9. В настоящее время существует множество программ, которые производят фильтрацию содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.
10. Не всей той информации, которая размещена в Интернете, можно верить.
11. Не оставляйте без присмотра компьютер с важными сведениям на экране.
12. Опасайтесь подглядывания через плечо.
13. Не сохраняйте важные сведения на общедоступном компьютере.

Приложение 4

Материалы для проведения родительского собрания

Анкета для родителей

Уважаемые родители! В школе информационные технологии применяются в различных направлениях: учебная деятельность (урочная и внеклассная), воспитательная (классные часы и различные школьные мероприятия), ИКТ являются основой единого информационного пространства школы (администрация школы,

учитель, ученик, родитель) - сайт школы, работа "Электронного журнала", учебно-материальная база школы, цифровые образовательные ресурсы и т.п. В том числе, информационные технологии прочно вошли в деятельность и досуг детей. Просим Вас ответить на несколько вопросов. (Все вопросы не являются обязательными для ответа. Если Вы выбираете "другое" - не забудьте написать свой ответ).

1. В каком классе учится Ваш ребенок?_____

2. ***Отношение к внедрению ИТ в образование.*** Внедрение информационных технологий (ИТ) в образование относится к числу крупномасштабных инноваций, пришедших в российскую школу в последние десятилетия. Среди ИТ, внедряемых в сфере образования, можно выделить следующие: обучающие, тренажеры, справочные, единые информационными образовательные пространства (сайт школы, дистанционное обучение, электронные дневники), техническое обеспечение кабинетов и др.

- скорее положительно
- скорее отрицательно (не вижу необходимости)
- другое:_____

3. ***Информационные технологии и обучение в школе.*** Проводятся различные мероприятия с применением информационных технологий (проектная деятельность, уроки, классные часы и родительские собрания).

- урок, с применением новых информационных технологий более популярен у моего ребенка (более интересен, понятен и т.п. - со слов ребенка)
- ребенок с интересом и удовольствием выполняет проекты (рефераты, доклады), используя компьютер
- ребенок готовится к уроку, используя компьютер (Интернет, полезные ссылки на сайте школы, рекомендуемые учителем сайты и т.п.)
- классный руководитель проводит родительские собрания с использованием компьютера
- другое:_____

4. ***Работа "Электронного журнала".*** Одной из возможностей ресурса является просмотр на страницах этого ресурса в Интернете оценок учащегося, которые выставляют учителя на уроках и их комментарии, домашнее задание... (пароль доступа индивидуален для каждого пользователя).

- в нашем классе есть "Электронный журнал", его работа очень важна для нас
- в нашем классе есть "Электронный журнал", но в его работе нет необходимости
- возможности "Электронного журнала" очень важные, но в нашем классе он не работает

- в нашем классе он не работает и думаю, что нет в нем необходимости
- другое:_____

5. ***Посещение Школьного сайта***

- часто посещаем (в том числе раздел Новости)
- очень редко посещаем
- не посещаем
- другое:_____

6. ***Школьный сайт.*** Напишите, пожалуйста, что бы Вы хотели изменить в работе сайта. Ваши предложения и рекомендации Вы можете написать в этом разделе!_____
_____

7. Есть ли у Вас дома компьютер?

- да (один)
- да (несколько)
- нет
- другое:

_

8. Кто пользуется компьютером у Вас дома?

- только родители
- только ребенок
- все члены семьи (родители и дети)

Примерный список вопросов, которые планируется обсудить на родительском собрании:

1. В каком возрасте следует разрешить детям посещение Интернета?
2. Следует ли разрешать детям иметь собственные учетные записи электронной почты?
3. Какими внутрисемейными правилами следует руководствоваться при использовании Интернета?
4. Как дети могут обезопасить себя при пользовании службами мгновенных сообщений?
5. Могу ли я ознакомиться с записью разговоров моего ребенка в программе обмена мгновенными сообщениями (MSN Messenger, ICQ, Mail Agent)?
6. Могут ли дети стать интернет-зависимыми?
7. Что должны знать дети о компьютерных вирусах?
8. Как проследить, какие сайты посещают дети в Интернете?
9. Что следует предпринять, если моего ребенка преследуют в Интернете?
10. Помогает ли фильтрующее программное обеспечение?
11. На какие положения политики конфиденциальности детского сайта нужно обращать внимание?
12. Какие угрозы встречаются наиболее часто?
13. Как научить детей отличать правду от лжи в Интернет?

Приложение 5

Рекомендации для родителей (законных представителей) детей различных возрастных категорий

Возраст от 7 до 8 лет

Находясь в Интернете, ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернету. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку. Запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security версии 7.0 со встроенным родительским контролем.

Советы по безопасности в сети Интернет:

Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля.

Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM).

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.

Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

Научите детей не загружать файлы, программы или музыку без вашего согласия.

Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

Подробнее о таких фильтрах

http://www.microsoft.com/rus/athome/security/email/fightspam.mspx.

Не разрешайте детям использовать службы мгновенного обмена сообщениями.

В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах.

Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте:

Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Не забывайте беседовать с детьми об их друзьях в Интернет.

Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.

Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Расскажите детям о порнографии в Интернет.

Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст от 13 до 17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте:

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут

грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет.

Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах).

Компьютер с подключением к сети Интернет должен находиться в общей комнате.

Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни.

Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

Приучите детей не загружать программы без вашего разрешения.

Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Расскажите детям о порнографии в Интернет.

Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

Приучите себя знакомиться с сайтами, которые посещают подростки.

Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Приложение 6

План - конспект урока на тему «Безопасный Интернет»

(9 – 11 класс)

Цель урока: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

- изучение информированности пользователей о безопасной работе в сети Интернет;
- знакомство с правилами безопасной работы в сети Интернет;
- ориентироваться в информационном пространстве; способствовать ответственному использованию online-технологий;
- формирование информационной культуры обучающихся, умения самостоятельно находить нужную информацию, пользуясь web-ресурсами;
- воспитание дисциплинированности при работе в сети. Обучающиеся должны знать:

➢ перечень информационных услуг сети Интернет;
➢ правилами безопасной работы в сети Интернет;
➢ опасности глобальной компьютерной сети.
➢ Обучающиеся должны уметь:
➢ ответственно относиться к использованию on-line-технологий;
➢ работать с Web-браузером;
➢ пользоваться информационными ресурсами;
➢ искать информацию в сети

Интернет. Тип урока: урок изучения нового материала.

Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично-поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

Ссылки на web-ресурсы:

1) http://www.kaspersky.ru – антивирус «Лаборатория Касперского»;
2) http://www.onlandia.org.ua/rus/ - безопасная web-зона;
3) http://www.interneshka.net – международный онлайн-конкурс по безопасному использованию Интернета;
4) http://www.saferinternet.ru – портал Российского Оргкомитета по безопасному использованию Интернета;

5) http://content-filtering.ru – Интернет СМИ «Ваш личный Интернет»;
6) http://www.rgdb.ru – Российская государственная детская библиотека.

Этапы урока:

1. Организация начала урока. Постановка цели урока. Просмотр видеоролика http://video.mail.ru/mail/illari.sochi/_myvideo/1.html. Постановка темы и главного вопроса урока.
2. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения обучающихся).
3. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.
4. Закрепление изученного материала. Рекомендации по правилам безопасной работы. Тестирование.
5. Подведение итогов урока. Оценка работы группы. Домашнее задание.

Ход урока

1. Организация начала урока. Постановка цели урока.

Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получили доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И никогда-то, а прямо сейчас.

(Просмотр видеоролика «Дети и Интернет» – (по выбору) (http://www.youtube.com); Как оставаться в безопасности на YouTube; Развлечения и безопасность в Интернете; Остерегайся мошенничества в Интернете; Мир глазами Gmail - ЗАЩИТА ОТ СПАМА).

Как не стать жертвой сети Интернет? Тема нашего урока - «Безопасный Интернет».

Главный вопрос урока: Как сделать работу в сети безопасной? 2. Изучение нового материала. Игра «За или против».

Учитель предлагает игру «За или против». На слайде - несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!
2. Интернет – это глобальный рекламный ресурс. И это хорошо!

3. Общение в Интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.

4. Интернет является мощным антидепрессантом.

5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Виртуальные грабли

Учитель предлагает обучающимся ответить на вопросы «Какие опасности подстерегают нас?», «Какие виртуальные грабли лежат у нас на пути?». (Целесообразно заранее нескольким обучающимся подготовить короткие сообщения по темам: «Интернет-зависимость», «Вредоносные и нежелательные программы», «Психологическое воздействие на человека через Интернет», «Материалы нежелательного содержания», «Интернет- мошенники»).

Физ. минутка «Собери рукопожатия».

Участникам предлагается в течение 10 секунд пожать руки как можно большего числа других людей.

Обсуждение.

- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Если – да, то чем он был вызван?

Анализ ситуации.

Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия? Однако, очень важно знать, что есть рядом люди, готовые выслушать, оказать поддержку, помочь в трудную минуту.

Учитель предлагает ответить на главный вопрос урока – «Как сделать работу в сети безопасной?»

3. Практическая работа.

Что можно? Что нельзя? К чему надо относиться осторожно?

Обучающимся предлагается посмотреть ресурсы http://content-filtering.ru/; http://www.microsoft.com/; http://www.youtube.com/

Учитель спрашивает, что об этом можно прочитать на web-страницах и просит обучающихся сформулировать правила безопасной работы.

Резюме (обсуждение найденной информации). Какие правила безопасной работы выбрали обучающиеся, посещая web-сайты?

4. Закрепление изученного материала.

Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые

простые рекомендации, используя хорошо известные образы.

Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо

бессмысленного блуждания по сети ваше Интернет-общение будет приносить пользу.

Рефлексия. На данном этапе предлагается подвести итоги урока Интернет-безопасности: на столе лежат три смайлика, обучающимся необходимо выбрать и положить перед собой тот, который соответствует настроению школьника.

И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

Оценивание обучающихся.

Информация о домашнем задании, инструкция о его выполнении:

1. Дать определение понятию «информационная безопасность».
2. Составить информационный лист «Моя безопасная сеть».

Приложение 7

Примерные материалы итогового анкетирования обучающихся по теме "Безопасный Интернет"

1. Укажите свой возраст_____
2. Что такое Интернет?_____
3. Какие опасности существуют в Интернете?_____

_____

4. Использование Интернета является безопасным, если: * выберите один или несколько вариантов из списка ответов

a) защитить свой компьютер, защитить себя в Интернете, соблюдать правила

b) разглашать личную информацию, заботиться об остальных, регулярно обновлять операционную систему защитить компьютер, создавать резервные копии документов, закону надо подчиняться даже в Интернете

5. Как защитить себя в Интернете? * выберите один или несколько вариантов из списка ответов

a) защитить свой компьютер, расширять круг знакомств с неизвестными людьми

b) стараться давать как можно меньше информации о себе

c) размещать фотографии свои, друзей и родственников

6. Как обезопасить свой компьютер? * выберите один вариант из списка ответов

a) выключить и спрятать в шкаф

b) установить антивирусную программу

7. Что надо делать, чтобы антивирусная программа была эффективной

*выберите один или несколько вариантов из списка ответов

a) лучше не иметь антивирусную программу

b) обновлять антивирусную базу

c) не посещать сайты, где нет достоверности, что сайт находится под защитой

8. Кто создаёт опасные программы? * выберите один или несколько вариантов из списка ответов

a) чёрный властелин

b) хакеры

c) шпионы

d) пожиратели смерти

9. Перечислите правила поведения в Интернете * если вы не знаете ответа на этот вопрос, то напишите "Без ответа"_____

10. А что для вас является "Безопасным Интернетом?" * если вы не знаете ответа на этот вопрос, то напишите "Без ответа"_____

Приложение 8

Полезные ссылки для подготовки и проведения круглых столов, диспутов, бесед и т.д. по вопросам профилактики преступлений в области компьютерных технологий среди несовершеннолетних

Адрес сайта	Содержание сайта
www.saferunet.ru	**Центр безопасного Интернета в России** Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Содержит практические советы, рекомендации по безопасности в сети.
www.mir.pravo.by/library/edu	**Детский правовой сайт** Содержит информацию о предупреждении правонарушений в Интернет–среде; причинах, способствующих возникновению компьютерной
	зависимости; правила безопасности для детей в Интернете и др.
www.ifap.ru/	**Безопасность детей в Интернете** На сайте можно получить информацию об опасности, которая таится во Всемирной паутине.

www.rusla.ru/	**Информационный портал школьных библиотек России** Содержит информацию о безопасном и более ответственном использовании онлайн-технологий, особенно среди детей и молодежи по всему миру.
www.wildwebwoods.org	**Игра для детей про безопасность в Интернете**
www.kaspersky.ru/	**Компьютерные угрозы. Интернет и дети** Сайт содержит информацию о защите ребенка при пользовании Интернетом.
www.saferinternet.ru	**Портал Российского Оргкомитета по проведению Года Безопасного Интернета** Сайт информирует о представителях всех ведущих общественных, некоммерческих и других организаций, деятельность которых связана с развитием безопасного Интернета. Содержит информацию о законодательстве в области компьютерных технологий.
www.nedopusti.ru	**Социальный проект «Не допусти»** На сайте указаны горячие линии помощи жертвам Интернет – угроз.
www.huliganam.net	**Социальный проект «Хулиганам.Нет»** Информирует о возможных незаконных действиях против личности в сети Интернет, методах борьбы с нарушителями.

Приложние 9

Рекомендации родителям по предупреждению компьютерной зависимости

1. Придерживайтесь демократического стиля воспитания в семье, который в наибольшей степени способствует воспитанию в ребенке самостоятельности, активности, инициативы и ответственности.

2. Не бойтесь показывать свои чувства ребенку, если Вы расстроены сложившейся «компьютерной» ситуацией. Тогда он увидит в Вас не противника, а близкого человека, который тоже нуждается в заботе.

3. Необходимо оговаривать время игры ребенка на компьютере и точно придерживаться этих рамок. Количество времени нужно выбирать, исходя из возрастных особенностей ребенка. Например, до 5 лет не рекомендуется

ребенка допускать до компьютера, стоит поощрять его познание мира без посредничества электроники. С 6 лет ребенку можно начинать знакомиться с компьютером (15-20 мин. в день). Для подростка 10-12 лет желательно не более 2 часов в день и не подряд, а по 15-20 минут

с перерывами.

4. Категорически запрещайте играть в компьютерные игры перед сном.

5. Необходимо прививать ребенку интерес к активным играм и физическим упражнениям (чтобы он чувствовал радость от этого), а также приобщать ребенка к домашним делам.

6. Необходимо следить, чтобы игра на компьютере не подменяла реальное общение со сверстниками, друзьями и близкими. Приглашать чаще друзей ребенка в дом.

7. Не нужно ограждать ребенка от компьютера вообще, поскольку это неотъемлемая часть будущего, в котором ребенку предстоит жить.

Литература

1. Асмолов А.Г. О смыслах понятия «толерантность» / А.Г. Асмолов, Г.У. Солдатова, Л.А. Шайгерова // Век толерантности: научно публицистический вестник. М., 2001, №1, С. 2-9.
2. Асмолов А.Г. Психология личности / А.Г. Асмолов, М.: Смысл, 2002;
3. Асмолов А.Г. Толерантность как культура XXI века / А.Г. Асмолов // Толерантность: объединяем усилия. М., 2002. С.18-25.
4. Бабаева Ю.Д., Одаренный ребенок за компьютером / Ю.Д. Бабаева, А.Е. Войскунский, М.: Сканрус, 2003.
5. Баева И.А., ред. Обеспечение психологической безопасности в образовательном учреждении / И.А. Баева, М., 2006.
6. Бурменская Г.В., Захарова Е.И., Карабанова О.А., Лебедева Н.Н., Лидерс А.Г. Возрастно-психологический подход в консультировании детей и подростков / Г.В. Бурменская, Е.И. Захарова, О.А. Карабанова, Н.Н. Лебедева, М., 2005.
7. Выготский, Л.С. Проблемы возрастной периодизации детского развития / Л.С. Выготский // Вопросы психологии, 1972, № 2, С. 3-12.
8. Дубровина И.В. Практическая психология образования в Психологическом институте / И.В. Дубровина // Вопросы психологии, 2004,№ 2, С. 4-11.
9. Кабаченко Т.С. Методы психологического воздействия / Т.С. Кабаченко, М.: Академия, 2000.
10. Коваль Т.В. Личностная сфера подростков, склонных к развитию компьютерной зависимости: Автореф. дис. канд. психол. наук / Т.В. Коваль, М., 2013.
11. Коркина А. Ю. Критерии психологической оценки компьютерных игр и развивающих компьютерных программ / А.Ю. Коркина // Психологическая наука и образование, 2008, № 3, С. 19-24.
12. Маслов О.Р. Психика и реальность: типология виртуальности / О.Р. Маслов, Е.Е. Пронина // Виртуальная

реальность. М.: Российская ассоциация искусственного интеллекта, 1998, С. 211 – 224.

13. Орлов А.Б. Психологическое насилие в семье – определение, аспекты, основные направления оказания психологической помощи / А.Б. Орлов // Журнал практического психолога, 2008, №4, С. 12-22.

14. Постман Н. Исчезновение детства / Н.Постман // Отечественные записки, 2004, № 3, С.7-15.

15. Прихожан А.М. Влияние электронной информационной среды на развитие личности детей младшего школьного возраста [Электронный ресурс]http://psystudy.ru/index.php/num/2010n1-9/283-prikhozhan9.html

16. Смирнова Е.О. Психологические особенности компьютерных игр: новый контекст детской субкультуры / Е.О. Смирнова, Р.Е. Радева // Образование и информационная культура. Социологические аспекты. Труды по социологии образования. Т.V, Вып. VII / Под ред. В. С. Собкина, М., 2000, С. 12-26.

17. Смирнова Е.О. Ребенок у экрана: чем опасны оковы телерабства / Е.О. Смирнова // Дошкольное воспитание. 2002, №7, С.4-11.

18. Чалдини Р. Психология влияния / Р. Чалдини, СПб.: Питер, 2001.

19. Эльконин Д.Б. К проблеме периодизации психического развития в детском возрасте / Д.Б. Эльконин // Вопросы психологии, 1971, № 4, С.3-9.

22. Эриксон Э. Детство и общество / Э. Эриксон, М.: Питер, 200